PKI-based Attestation Evidence

Mike Ounsworth , Richard Kettlewell , Jean-Pierre Fiset , Hannes Tschofenig , Tirumaleswar Reddy.K , Monty Wiseman

Status

- Draft became WG item recently
- Document describes encoding of evidence claims in ASN.1/DER format.
- Content is based on the EAT specification + HSM-specific evidence (FipsMode, PubKey, Purpose, NonExportable, Imported, KeyExpiry).

Problem – transcoding EAT submods claim into ASN.1

- Fact: the EAT submods CDDL is incredibly complex because it handles all combinations of:
  - CWT-inside-CWT
  - JWT-inside-JWT
  - CWT-inside-JWT
  - JWT-inside-CWT
- Transcoding the CDDL for `submods` to ASN.1 is not straightforward.
- Moreover, once we have an ASN.1 encoding of EAT then `submods` will have in theory 3*3 = 9 combinations to consider.

Problem – transcoding EAT submods claim into ASN.1

- Thomas Fossati suggested that a layer of abstraction solves all problems.
  1. Define a way to put an ASN.1 EAT inside a CMW.
  2. Define ASN.1 EAT submods claim to accept a CMW.
- This would handle the {cwt,jwt}-in-ASN.1 cases, but not the ASN.1-in-{cwt,jwt} cases.
- Proposed ASN.1 here:
  - https://github.com/ietf-rats-wg/draft-ietf-rats-msg-wrap/wiki/CMW-in-ASN.1
- (authors have not yet considered this in detail)

Hackathon example

Showing 3 claims in a signed data structure.

```
  0 179: SEQUENCE {
  3 102:   SEQUENCE {
  5   1:     INTEGER 1
  8  81:     SEQUENCE {
 10  36:       SEQUENCE {
 12   6:         OBJECT IDENTIFIER Hwmodel Claim (1 1 1 1 1 1 1)
     :           (Hwmodel)
 20  26:         UTF8String 'Crypto4A HSM Example Model'
     :         }
 48  13:       SEQUENCE {
 50   6:         OBJECT IDENTIFIER Hwversion Claim (1 1 1 1 1 1 2)
     :           (Hwversion)
 58   3:         UTF8String '1.0'
     :         }
 63  26:       SEQUENCE {
 65   6:         OBJECT IDENTIFIER Hwserial Claim (1 1 1 1 1 1 3)
     :           (Hwserial)
 73  16:         UTF8String '20230715-001-123'
     :         }
     :       }
 91  14:     SEQUENCE {
 93  12:       SEQUENCE {
 95  10:         SEQUENCE {
 97   8:           OBJECT IDENTIFIER ECDSA with SHA-256 (1 2 840 10045 4 3 2)
     :             (ecdsa-with-SHA256)
     :           }
     :         }
     :       }
     :     }
107  73:   SEQUENCE {
109  71:     BIT STRING, encapsulates {
112  68:       SEQUENCE {
114  32:         INTEGER
     :           26 3F F0 2F FC 8D A5 D9 B4 D5 27 61 D9 59 BF 6A
     :           D9 D8 8F 4B F0 78 FC 15 D7 0A 84 C1 B5 91 5C C4
148  32:         INTEGER
     :           19 4D F8 D0 3B 86 0B 68 C2 29 70 6D 64 97 9F 6C
     :           26 9D 4F 40 60 F3 39 FA B3 C2 53 82 7E 16 E5 23
     :         }
     :       }
     :     }
     :   }
```

Proposed Next Steps

- Split document into two:

1. Encoding of EAT claims in ASN.1/DER as Evidence
2. Key Attestation Architecture and encoding of key attestation claims in ASN.1/DER & EAT format

- Another document about encoding of Attestation Results in X.509 certificates.